CS 370: Introduction to security

04.04: Course introduction

Tu/Th 4:00 – 5:50 PM (WNGR 149)

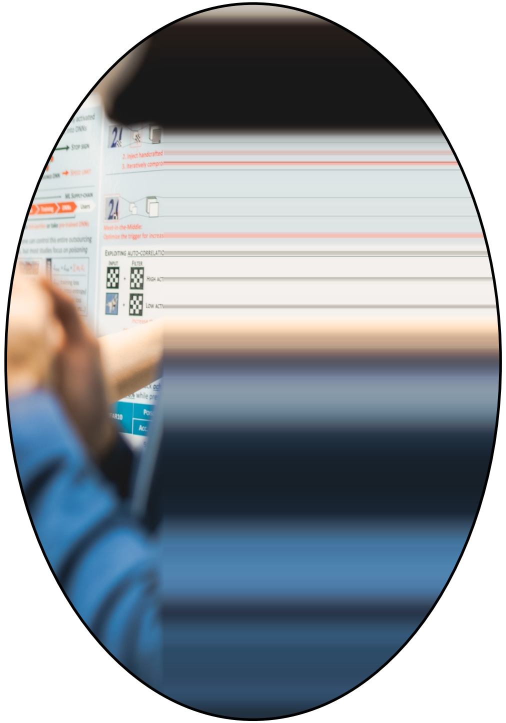
Sanghyun Hong

sanghyun.hong@oregonstate.edu

Oregon State University

SAIL
Secure AI Systems Lab

Instructor: Sanghyun Hong



Who am I?

- **2021 - Now:** Assistant Professor of Computer Science at OSU
- **2021:** Ph.D. from the University of Maryland, College Park
- **2015:** B.S. from Seoul National University, South Korea

What I do?

- **Formal:** I work at the intersection of security, privacy, and machine learning
- **Informal:** I am an “AI-hacker”

What do I teach?

- CS 344: OS I | CS 370: Introduction to Security
- CS 499/579: Trustworthy ML | CS 578: Cyber-security

Where can you find me?

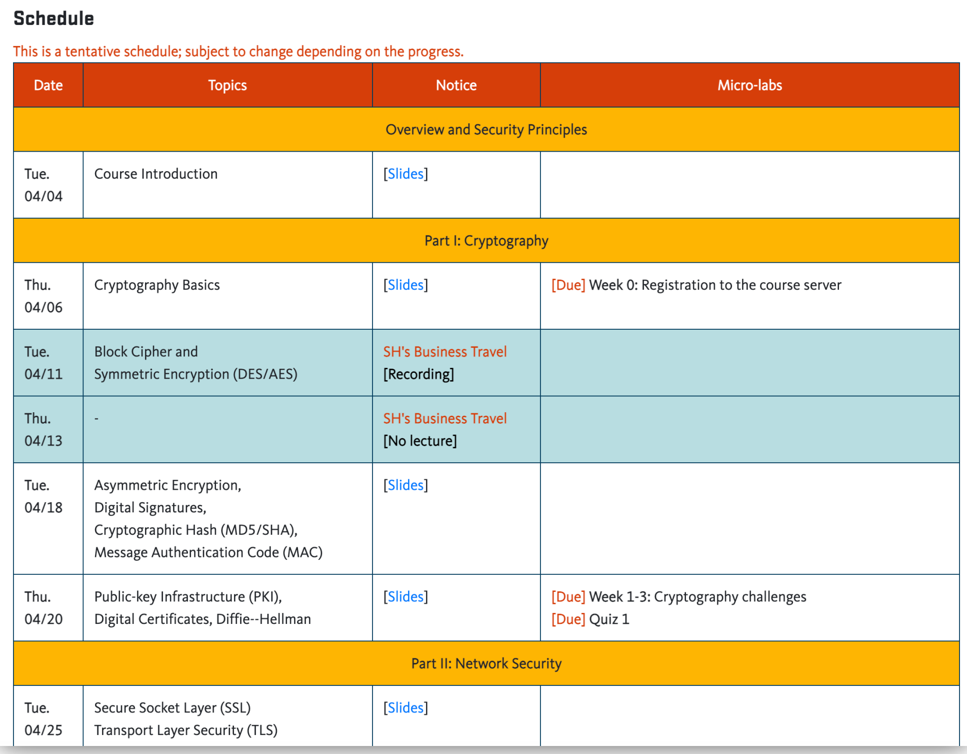
- **Office:** #4103 Kelley Engineering Center (KEC)
- **Email:** sanghyun.hong (at) oregonstate.edu | Discord Server
- **Website:** sanghyun-hong.com (drop me an email if you want to do research)

Goals (learning objectives)

- Here are (but let's add more if we want to)
  - Why do we care about computer security?
  - What are the basic principles of computer security?
  - What are the areas of computer security (and research!)?
  - …

Course structure

- 10-week lecture topics
  - W1-3: Cryptography
  - W4-5: Network security
  - W5-6½: Internet security
  - W6½-8: Software security
  - W9: Trustworthy ML
  - W10: Usable security and privacy
- Micro-labs
  - Understand core sec. concepts
  - Hands-on (micro) practices
  - … Ethical hacking
- 3 Quizzes



Schedule

This is a tentative schedule; subject to change depending on the progress.

Date	Topics	Notice	Micro-labs
Overview and Security Principles			
Tue. 04/04	Course Introduction	[Slides]	
Part I: Cryptography			
Thu. 04/06	Cryptography Basics	[Slides]	[Due] Week 0: Registration to the course server
Tue. 04/11	Block Cipher and Symmetric Encryption (DES/AES)	SH's Business Travel [Recording]	
Thu. 04/13	-	SH's Business Travel [No lecture]	
Tue. 04/18	Asymmetric Encryption, Digital Signatures, Cryptographic Hash (MD5/SHA), Message Authentication Code (MAC)	[Slides]	
Thu. 04/20	Public-key Infrastructure (PKI), Digital Certificates, Diffie--Hellman	[Slides]	[Due] Week 1-3: Cryptography challenges [Due] Quiz 1
Part II: Network Security			
Tue. 04/25	Secure Socket Layer (SSL) Transport Layer Security (TLS)	[Slides]	

…

Important information

- Overview
  - 4 credit courses: 12+ hours of effort per week
  - Couse website: https://secure-ai.systems/courses/Sec-UGrad/Sp23
- Contacts:
  - Me: sanghyun.hong@oregonstate.edu
    - Office hours: W 5:30 – 7 pm (on Zoom: link is available on Canvas)
  - Awesome TAs
    - Eunjin Roh (rohe@oregonstate.edu)
    - Hayden Johnson (johnhayd@oregonstate.edu)
    - No office hours in the first week (we're finalizing our schedules)
    - Zoom links will be available on Canvas once we set our office hours
  - Micro-labs: http://ctf.secure-ai.systems
- Discussion
  - On Discord server or ChatGPT?

Grading (subject to change)

- Portions
  - **70%:** Micro-labs
  - **30%:** Quizzes 1-3
    - Quiz 1: Cryptography basics
    - Quiz 2: Network and internet security
    - Quiz 3: Software security, trustworthy ML, and usable security/privacy
    - Note:
      - 60-min, on Canvas
      - 3 trials possible, and the best will be taken
  - **TBD%:** Extra credit opportunities
    - **+2%:** Practice of using E2EE
    - …

Grading (subject to change)

- Grading cheme
  - A >= 93%
  - A- >= 90%
  - B+ >= 87%
  - B >= 83%
  - B- >= 80%
  - C+ >= 77%
  - C >= 73%
  - C- >= 70%
  - D+ >= 67%
  - D >= 63%
  - D- >= 60%
  - F < 60%

Micro-labs (70%)

- 6 Sets on 6 topics
  - Set 1: Cryptography
  - Set 2: Network security
  - Set 3: Internet security
  - Set 4: Software security
  - Set 5: Trustworthy ML
  - Set 6: Usable security/privacy

Micro-labs (70%)

- 6 Sets on 6 topics
  - Set 1: Cryptography
    - How to encrypt data
    - How to break “some” crypto schemes
    - How to break digital signatures
    - How authentication can go wrong
  - Set 2: Network security
  - Set 3: Internet security
  - Set 4: Software security
  - Set 5: Trustworthy ML
  - Set 6: Usable security/privacy

Micro-labs

- Micro-lab instructions
  - CTF-style system: lab server, instructions
  - CTF-solve server: solve.secure-ai.systems (under maintenance; announce the instructions to use it soon)

Micro-labs

- Micro-lab instructions
  - CTF-style system: lab server, instructions
  - Rules:
    - **Do not** share your code with other students (how-it-can-trigger-me)
      - **Encouraged to discuss** with others about the assignments
      - **Do not** ask/give the code to others
      - **Do not** copy other students' code or code available in online
      - **Do not** publish your code online
    - You will be asked to submit a simple write-up for the assignment
      - Describe how you solve each challenges
      - **Mention your collaborators** in the write-up
      - **Do not** copy other students' write-up
      - **Do not** publish your write-up online

Micro-labs

- Micro-lab instructions
  - CTF-style system: lab server, instructions
  - Rules (collapsed; see the previous slide)
  - Broken… then:
    - Plagiarism will be punished via the Office of Student Life
      - Getting F or zero score for the labs that matters with plagiarism
    - Code of Student Conduct
      - https://studentlife.oregonstate.edu/studentconduct/academicmisconduct
      - https://studentlife.oregonstate.edu/sites/studentlife.oregonstate.edu/files/edited_code_of_student_conduct.pdf

Micro-labs

- Micro-lab instructions
  - CTF-style system: lab server, instructions
  - Rules (collapsed; see the previous slide)
  - Broken… then (collapsed; see the previous slide)
  - **Due dates are on the course website**
    - Deadline will be at 11:59:59 PM on each due date

Micro-labs

- Micro-lab instructions
  - CTF-style system: lab server, instructions
  - Rules (collapsed; see the previous slide)
  - Broken… then (collapsed; see the previous slide)
  - **Due dates are on the course website**
    - Deadline will be at 11:59:59 PM on each due date
    - But late submissions are possible until the end of this term (with 50% deduction)
  - Grading policy
    - **100% score:** Submission before the due date
    - Late submissions
      - 5% deduction / day: Submissions passed the due date
      - 50% deduction at max.

Others

- Let’s help each other (on Discord)
  - But do not share your code directly
  - It’s not a “help”; it will ruin your friend’s career
  - Do encourage and guide them to the solutions
- Let’s “also” have fun!

Thank You!

Tu/Th 4:00 – 5:50 PM (WNGR 149)

Sanghyun Hong

sanghyun.hong@oregonstate.edu

Oregon State University

SAIL

Secure AI Systems Lab